In the claims:

The following listing of claims will replace all prior listings and versions of the claims.

1. (Currently amended) A method of providing a key container by a key container directory, the key container to be used to secure a message that will be sent from a sender to a recipient, the method comprising the steps of:

receiving a request for [[the]] a key container and authentication credentials from a requestor; and

in response to the request, determining the type of key container that should be provided to the requestor based on the authentication credentials and providing a key container of the determined type to the requestor ~~that contains~~ containing a cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

2. (Currently amended) A method of providing a key container according to claim 1, wherein the key container directory is remote from the gateway~~, such as external to the network domain of the gateway~~.

3. (Previously presented) A method of providing a key container according to claim 1, wherein the key container directory is external to the network domain of the recipient.

4. (Currently amended) A method of providing a key container according to claim 1, wherein the message is transmitted from the sender over an insecure computer network~~, such as the Internet~~.

5. (Previously presented) A method of providing a key container according to claim 1, wherein the network domain of the recipient is secure.

6. (Currently amended) A method of providing a key container according to claim 1, wherein the step of providing a key container of the determined type comprises providing [[a]] key containers ~~container for each gateway~~ that each contain a cryptographic key for a gateway the message will transit.

7. (Previously presented) A method of providing a key container according to claim 1, wherein the method further comprises the step of determining the identity of one or more gateways that the message will transit.

8. (Currently amended) A method of providing a key container according to claim 1, wherein the key container directory provides multiple key containers in [[the]] response to the request.

9. (Previously presented) A method of providing a key container according to claim 1, wherein the requestor is the sender of the message and the request includes the address of the recipient.

10. (Currently amended) A method of providing a key container according to claim 9, wherein the step of requesting [[the]] a key container includes an indication that an encryption key container is requested.

11. (Cancelled)

12. (Currently amended) A method of providing a key container according to ~~claims 11~~ claim 1, wherein the step of determining comprises in the event ~~determining whether~~ the requestor is the sender of the message~~, and if so,~~ providing an encryption key container to the requestor.

13. (Cancelled)

14. (Currently amended) A method of providing a key container according to claim [[11]] 1, wherein the step of determining further comprises determining whether the requestor is from the same domain as the gateway, and if so, providing the encryption key container having the cryptographic key of the requestor's gateway; and if not, providing the encryption key container containing the cryptographic key of the recipient's gateway.

15. (Previously presented) A method of providing a key container according to claim 1, wherein the requestor is the gateway and the request includes the address of the sender.

16. (Currently amended) A method of providing a key container according to claim 1, wherein the step of requesting [[the]] a key container includes an indication that a signing key container is requested.

17. (Cancelled)

18. (Currently amended) A method of providing a key container according to claim [[17]] 1, wherein the step of determining further comprises in the event ~~determining whether~~ the requestor is the gateway~~, and if so,~~ providing the signing key container containing the cryptographic key of the gateway and the message sender's address.

19. (Previously presented) A method of providing a key container according to claim claim 18, wherein the sender's address is from the same domain as the gateway.

20. (Currently amended) A method of providing a key container according to claim [[11]] 1, wherein the step of determining is based on parameters associated with the request.

21. (Previously presented) A method of providing a key container according to claim 1, wherein the method further comprises the step of the requestor authenticating with the key container directory.

22. (Currently amended) A method of providing a key container according to claim 21, wherein ~~the method further comprises the step of the requestor authenticating with the key container directory and the step of determining is based on the information provided by~~ the authentication credentials are received from the requestor when authenticating with the key container directory

23. (Previously presented) A method of providing a key container according to claim 21, wherein the step of authenticating is through the use of a valid username and password combination.

24. (Previously presented) A method of providing a key container according to claim 1, wherein once the request has been received, the method further comprises the step of generating the requested key container.

25. (Previously presented) A method of providing a key container according to claim 1, wherein the request is made using a computer communication protocol selected from the group consisting of Lightweight Directory Access Protocol (LDAP), Directory Access Protocol (DAP), Certification Management Protocol (CMP), XML Key Management Specification (XKMS), and HyperText Transfer Protocol (HTTP).

26. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided contains a cryptographic key that is a public key.

27. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided is a digital certificate.

28. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided is a Pretty Good Privacy (PGP) public key.

29. (Previously presented) A method of providing a key container according to claim 1, wherein the address contained in the key container is an e-mail address and the gateway is an e-mail gateway.

30. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided is provided for a specific message.

31. – 32. (Cancelled)

33. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided contains the same container identifiers of the key container of the gateway.

34. (Previously presented) A method of providing a key container according to claim 1, wherein the key container that is provided is an encryption key container to be used for encryption operations.

35. (Currently amended) A method of providing a key container according to claim 34, wherein the key container that is provided contains a parameter that indicates that the key container is to be used for encryption functions.

36. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided secures the message through use of the cryptographic key to encrypt the message.

37. (Previously presented) A method of providing a key container according to claim 1, wherein the sender's address is from the same domain as the gateway.

38. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided is a signing key container.

39. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided contains a parameter that indicates that the key container is to be used for signing operations.

40. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided secures the message by being carried with the message.

41. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided includes information that permits a requestor to determine the authenticity and integrity of the key container.

42. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided contains security preferences of the gateway.

43. (Currently amended) A method of providing a key container according to claim 1, wherein the key container that is provided includes information about the key container directory that provided the key container.

44. (Previously presented) A key container directory operable to provide a key container according to the method of claim 1, wherein the key container directory is remote from the gateway.

45. (Original) A key container directory according to claim 44, wherein the key container has a datastore of cryptographic keys that can be contained in any provided key container.

46. – 66. (Cancelled)

67.[1] (New) A method of providing a key container according to claim 1, wherein the step of determining comprises in the event the requestor is anonymous, the determined type of container is an encryption key container.

[1] In the August 22, 2007 Preliminary Amendment, claims 67-69 were cancelled. It appears, however, that that was a mistake as no claims 67-69 appear to have been present in the underlying priority application, the PCT application on which the present application is based, or anywhere else in this application. Therefore, the next claim number in the sequence should be 67.